Date: 03/02/2025

1. IT Asset Management
2. Vulnerability
3. Obsolescence
4. Complaince
5. Maintenance
6. End of Life
7. End of Support
8. End of Maintenance
9. Asset Hygiene
10. Crown Jewel
11. Inventory
12. NVD
13. Patch Management

1. IT Asset Management (ITAM)

🔷 **Meaning:**

IT Asset Management (ITAM) is the process of **tracking, managing, and optimizing IT assets** (hardware, software, licenses, cloud resources) to ensure they are efficiently used, secured, and compliant.

🔷 **Key Aspects:**

- **Asset Lifecycle Management** – From procurement to disposal.
- **Inventory Tracking** – Keeping records of all IT assets.
- **Cost Optimization** – Avoiding unnecessary expenses on licenses or hardware.
- **Compliance & Security** – Ensuring proper software licensing and data protection.

🔷 **Example:**

A company uses an ITAM tool like **ServiceNow or Lansweeper** to monitor all laptops, desktops, and software licenses, ensuring compliance with software vendors like Microsoft and Adobe.

---

2. Vulnerability

🔷 **Meaning:**

A vulnerability is a **flaw or weakness** in an IT system that attackers can exploit to compromise security.

🔷 **Key Aspects:**

- **Software Bugs** – Programming errors (e.g., buffer overflow).
- **Misconfigurations** – Weak security settings (e.g., open ports).
- **Zero-Day Vulnerabilities** – Unknown flaws not yet patched.
- **Exposure to Attacks** – Malware, phishing, unauthorized access.

🔷 **Example:**

A **web application vulnerability (SQL Injection)** allows hackers to access customer data by injecting malicious SQL commands.

---

3. Obsolescence

🔷 **Meaning:**

Obsolescence occurs when **hardware or software becomes outdated**, leading to inefficiencies, compatibility issues, and security risks.

🔷 **Key Aspects:**

- **Planned Obsolescence** – Vendors discontinue support (e.g., Windows XP EOL).
- **Technological Advancements** – Newer software makes older versions redundant.
- **Security Risks** – Older systems don't receive updates, making them vulnerable.

🔷 **Example:**

A company still using **Windows 7** faces cybersecurity risks because **Microsoft no longer provides updates**.

---

4. Compliance

🔷 **Meaning:**

Compliance refers to **adhering to regulatory, legal, and security standards** set by industry bodies or governments.

🔷 **Key Aspects:**

- **Regulatory Standards** – GDPR (Data Protection), HIPAA (Healthcare), PCI-DSS (Payments).
- **Audits & Reporting** – Organizations must prove compliance through documentation.
- **Fines & Legal Consequences** – Non-compliance can result in financial penalties.

🔷 **Example:**

A bank must comply with **PCI-DSS regulations** to ensure secure credit card transactions.

---

5. Maintenance

🔷 **Meaning:**

IT maintenance involves **regular updates, monitoring, and troubleshooting** to keep systems running smoothly.

🔷 **Key Aspects:**

- **Preventive Maintenance** – Regular updates, patches, performance monitoring.
- **Corrective Maintenance** – Fixing software bugs or hardware failures.
- **Adaptive Maintenance** – Updating systems to meet changing needs.

🔷 **Example:**

A company **updates its firewall rules and antivirus software** monthly to prevent cyber threats.

---

6. End of Life (EOL)

🔷 **Meaning:**

EOL refers to the phase when **a vendor stops selling, supporting, and maintaining a product**.

🔷 **Key Aspects:**

- **No More Updates or Patches** – Security risks increase.
- **No Vendor Support** – Customers must migrate to newer versions.
- **Discontinuation Risks** – Lack of compatibility with modern tools.

🔷 **Example:**

Windows XP reached **EOL in 2014**, meaning Microsoft stopped providing security updates, making it vulnerable to cyberattacks.

---

7. End of Support (EOS)

🔷 **Meaning:**

EOS happens when a vendor **stops providing technical support**, but the product may still function.

🔷 **Key Aspects:**

- **No More Customer Service or Troubleshooting**.
- **Limited Support from Third-Party Vendors**.
- **Security Risks Due to Lack of Patches**.

🔷 **Example:**

A company using **Oracle Database 11g** after its **EOS date** must migrate to **Oracle 19c** for ongoing support.

---

8. End of Maintenance (EOM)

🔷 **Meaning:**

EOM is when a product stops **receiving regular maintenance**, but **limited support** may still be available.

🔷 **Key Aspects:**

- **Bug fixes and feature updates stop**.
- **Extended support may still be available at extra cost**.
- **System performance and security can degrade**.

🔷 **Example:**

A company using an **old CRM system** finds that while they can still use it, the vendor **no longer provides fixes or performance updates**.

Key Takeaways:

- **EOL** → Product is **discontinued completely** (no updates, no support, no sales).
- **EOS** → Product is **functional but lacks vendor support** (can still be used).

- **EOM** → Product **works but no longer gets fixes or improvements** (may still have limited support options).

9. Asset Hygiene

🔷 **Meaning:**

Asset Hygiene refers to maintaining **updated, secure, and properly managed IT assets**.

🔷 **Key Aspects:**

- **Regular Patching & Updates**.
- **Removing Unused or Unauthorized Software**.
- **Tracking Asset Usage to Avoid Waste**.

🔷 **Example:**

A company **removes outdated, unused applications** from employee laptops to prevent security risks.

---

10. Crown Jewel

🔷 **Meaning:**

Crown Jewels are **critical IT assets that, if compromised, could severely impact business operations**.

🔷 **Key Aspects:**

- **Highly Valuable Data** – Customer PII, intellectual property.
- **High-Level Security Measures** – Encryption, access control.
- **Disaster Recovery Planning** – Backups, incident response strategies.

🔷 **Example:**

A healthcare company's **patient database** is a **Crown Jewel**, requiring strict protection against breaches.

---

11. Inventory

🔷 **Meaning:**

IT inventory is a **catalog of all IT assets** (hardware, software, cloud resources) owned by an organization.

🔷 **Key Aspects:**

- **Helps in Asset Tracking & Budgeting**.
- **Prevents Unauthorized IT Usage**.
- **Essential for Compliance Audits**.

🔷 **Example:**

A business maintains a **cloud inventory** to monitor **AWS, Azure, and Google Cloud resources**.

---

12. NVD (National Vulnerability Database)

🔷 **Meaning:**

NVD is a **public database maintained by NIST** that catalogs software and hardware vulnerabilities.

🔷 **Key Aspects:**

- **Contains CVE (Common Vulnerabilities & Exposures)**.
- **Provides CVSS (Common Vulnerability Scoring System) Ratings**.
- **Used by Security Teams to Patch Systems**.

🔷 **Example:**

A cybersecurity team **monitors NVD** for newly disclosed vulnerabilities in **Windows Server** and applies patches accordingly.

---

13. Patch Management

🔷 **Meaning:**

Patch Management is the process of **identifying, testing, and applying updates (patches) to software and systems**.

🔷 **Key Aspects:**

- **Fixes Security Vulnerabilities**.
- **Improves Software Stability & Performance**.
- **Automated Patch Deployment Tools Help (WSUS, SCCM, etc.)**.

🔷 **Example:**

A company **deploys Microsoft Patch Tuesday updates** every month to fix known vulnerabilities.